

Information Warfare: Task Force XXI or Task Force *Smith*?

by Major Curtis A. Carver Jr., US Army
Copyright 1997

THE US ARMY is on the verge of suffering its greatest defeat in history—a defeat that will redefine revolution in military affairs on the informational battlefield. Why will this defeat occur you ask? Because the United States is not taking the defensive steps necessary to limit the effectiveness of a sophisticated, coordinated cyberwar attack, despite the availability of proper tools. This article examines the growing potential for an informational disaster by exploring recent cyberwar attacks and the threats posed by these attacks. After winning the first information-age war in the Persian Gulf, the United States could well be the next victim of information warfare.

The Challenge

Information warfare (IW) is not a new phenomenon but rather an ancient one that is rapidly growing and transforming due to the impact of technology. Sun Tzu succinctly characterized the goal of IW with his observation that “To win a hundred victories in a hundred battlefields is not the acme of skill, but to subdue the enemy without fighting is the acme of skill.”¹ Carl von Clausewitz likewise recognized IW’s importance, noting that “Knowledge must become capability.”² The 2nd Punic War, the Mongol Doctrine of the 13th century, the Sepoy Mutiny, the Normandy Invasion and Operation *Desert Storm* are all historical examples of IW’s dominant use.³ Because IW is as old as man himself, and given this rich heritage of historical IW, one may wonder why IW is receiving so much recent attention. The reason is the exploding impact of technology on IW.

Advances in technology are transforming IW by providing vastly improved capabilities, attainment of significant warfighting capabilities at relatively

Rogue nations with experienced, well-financed cyber warriors can attack with virtual immunity. Using Trojan Horse versions of programs, hackers can mask process activity, secondary storage and network protocol usage so as to withstand checksum and file-size integrity checks. System administrators will not even know they have been compromised. Unlike the telltale remains of a physical terrorist bomb, there are no bomb fragments in cyberwar, no log of events that can be linked to the attacking nation and no fear of reprisal.

low cost and fundamentally different tools and targets. Because the technologies of range—jet and rocket engines, cruise missiles—tend to improve slowly and are extremely expensive, the US advantage in these areas is relatively secure, while those based on information technologies are constantly threatened by an explosive technological revolution.⁴ Computer technology increases twofold every 18 months. Between 1981 and 1993, PC processor speeds increased 120-fold, from 250,000 to 30,000,000 instructions per second. Therefore, significant computational power is readily available at very low cost. Computer networks are growing at an even faster rate. Between 1981 and 1996, the Internet grew from 215 hosts and 56-kilobits-per-second (kbps) links to tens of millions of hosts and billions of bps links.⁵

Like the movement from wooden-hulled to steel-hulled warships in the 19th century, niche competitors of the United States view this technolo-

gical explosion as a means of leveling the playing field inexpensively and quickly. Hostile nations can buy the latest information technology at relatively low cost and rapidly become an IW military power. While no nation has exploited this opportunity, a recent review of cyberwar attacks starkly demonstrates the depth of America's growing vulnerability.

The IW threats facing the United States are growing and becoming increasingly sophisticated. In November 1988, Cornell University student Robert Morris inadvertently released the "Internet Worm." In the next two days, this poorly written 123-line program infected over 6,000 computer systems.⁶ The result: the Internet grinds to halt in the first and only successful attack against it. In August 1992, two graduate students at Texas A&M University uncovered a sophisticated, covert attempt to take over all of the mini- and mainframe computer systems at the university. Deeper investigation revealed that the attackers had already compromised the security of over 300 mini- and mainframe computer systems internationally and the computer hackers were using this tremendous computational power in an attempt to infiltrate numerous additional computer systems. The attacks were well coordinated, thorough and very sophisticated. In 1993, it was discovered that thousands of computer systems had been compromised through a "sendmail Trojan Horse." An unknown assailant had breached millions of user accounts and their associated E-mail accounts.⁷ Countless other uncoordinated attacks, such as the *Cuckoo's Egg*, *Argentine Intrusion* and *Rome Laboratory*, vividly demonstrate the potential for attacking the United States through cyberwar.⁸

As more and more people use computers and Internet computer networks, cyberwar attacks will grow dramatically in number and sophistication. The Defense Information Systems Agency (DISA) estimates that as many as 250,000 attacks may have occurred in 1995. Hackers attack Wright Patterson Air Force Base 3,000 to 4,000 times per month.⁹ Julio Ardita, *Argentine Intrusion* perpetrator, attacked over 367 sites a total of 836 times from the time he was first detected until he was caught.¹⁰

The number of attacks is rapidly becoming unmanageable for the typical system administrator. Moreover, sophisticated automated tools with user-friendly interfaces allow novices to attack and rapidly exploit systems without a real understanding of

how the attack is delivered. No longer is an in-depth knowledge of computers, operating systems, network protocols and computer networks a requirement for launching a successful attack. Tools such as *Cops* and *Crack* quickly find passwords, file

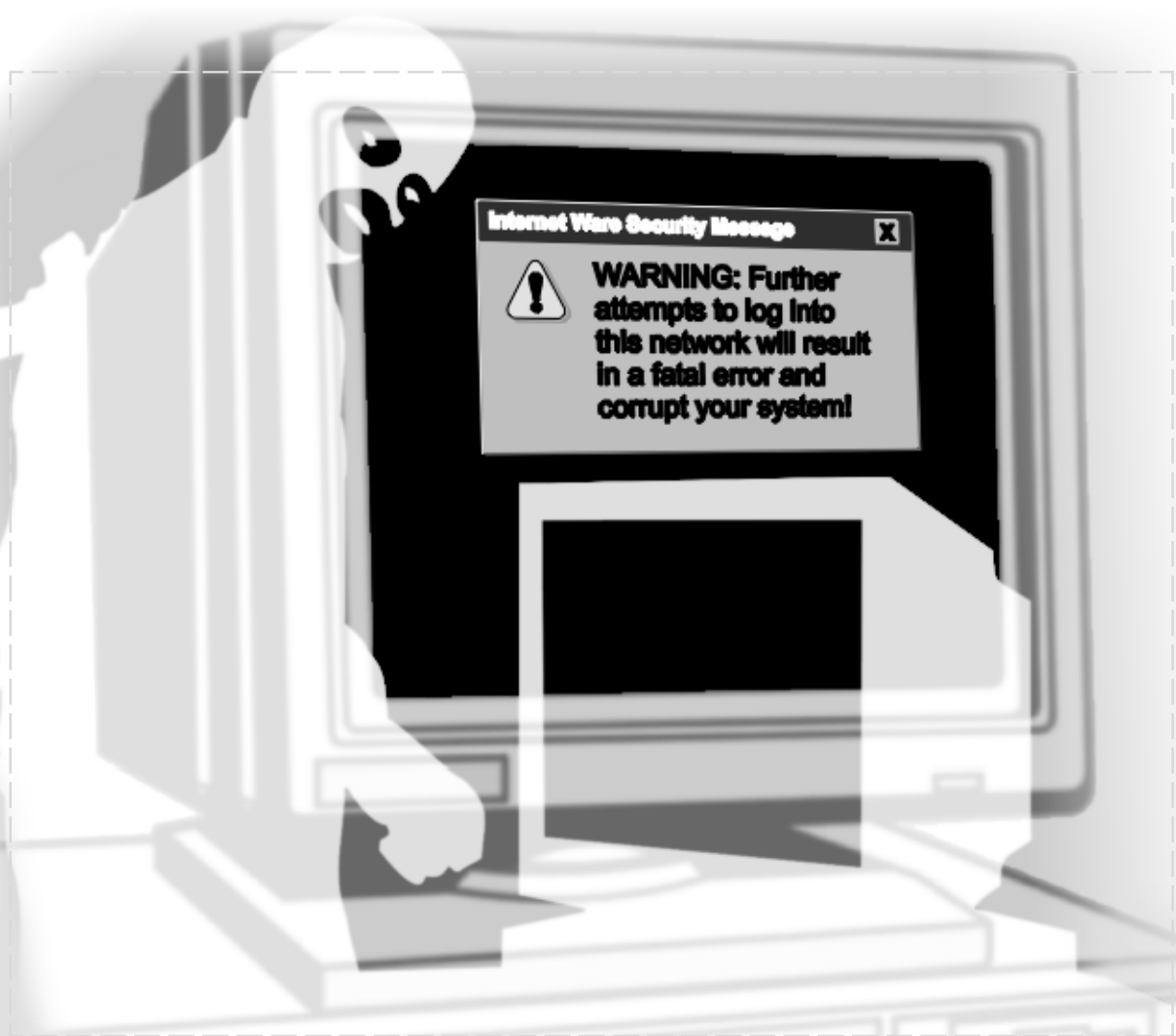
Because the technologies of range—jet and rocket engines, cruise missiles—tend to improve slowly and are extremely expensive, the US advantage in these areas is relatively secure, while those based on information technologies are constantly threatened by an explosive technological revolution. . . . Niche competitors of the United States view this technological explosion as a means of leveling the playing field inexpensively and quickly. . . . While no nation has exploited this opportunity, a recent review of cyberwar attacks starkly demonstrates the depth of America's growing vulnerability.

structure permissions and process weaknesses that hackers can exploit to gain access to a system and eventually gain "superuser" access to the computer system.¹¹ Knowledge is no longer a barrier to cyberwar: intent, a \$2,000 computer and a network connection are the only prerequisites.

Finally, hostile intent is abundant. The United States has numerous enemies unable to effectively challenge it on the physical battlefield, yet ready to exploit the potential of a decisive attack on the cyber-battlefield. Nations such as Iraq, Iran, North Korea, China, Libya and countless others can effectively bypass the overwhelming Maginot Line of traditional US defenses and attack directly at our digital infrastructure.¹² Due to fundamental weaknesses in information authentication and authorization, as well as its dependence on information, the United States is the nation most vulnerable to an attack—an attack similar to Pearl Harbor that will occur on American soil and will have devastating impact.

Fundamental Weaknesses

The United States is susceptible to a well-coordinated cyberwar attack due to fundamental weaknesses in computer authentication, network protocols and encryption. *Computer authentication* is the identification and verification of the user and is a key security weakness.¹³ Most computer authentication systems are limited to a simple log-in name and password. If a computer attacker can gain



The United States is susceptible to a well-coordinated cyberwar attack due to fundamental weaknesses in computer authentication, network protocols and encryption. Computer authentication is the identification and verification of the user and is a key security weakness. Most computer authentication systems are limited to a simple login name and password. If a computer attacker can gain access to a user's password and login, the hacker has access to all of the user's files and resources.

access to a user's password and login, the hacker has access to all of the user's files and resources. The attacker can then use the additional computational resources to attack other computer systems. Because most systems allow the user to choose the password or easily change it, users can introduce significant vulnerabilities into any computer system. Using common tools such as *Crack*, computer novices can automatically attack all of the user accounts on a computer system with over 300-rule-based attacks in as many languages as the attacker chooses. Computer scientists at the US Military Academy, West Point, New York, were consistently able to

infiltrate over 30 percent of their users' computer accounts by employing this simple but effective tool.¹⁴

Even though technologies such as public key digital signatures, one-time password devices, system-generated passwords and biometric devices—retinal scan, hand geometry and face recognition—exist, are commercially available and inexpensive, the vast majority of computer systems in the United States simply do not employ these security measures, leaving the computer systems extremely vulnerable to intrusion.¹⁵ More robust client-server authentication systems such as *Kerberos* and *SPX*

are likewise in limited use.¹⁶ We have the tools to protect ourselves but have decided not to. Like the situation before Pearl Harbor, we have the capability to protect ourselves but have chosen to discount the possibility of an attack. This failure to properly defend against possible hostile foreign attack could have dire consequences for the United States in the not-too-distant future.

In addition to the ease of automation infiltration, hackers and rogue nations launching cyberwar attacks enjoy almost complete anonymity due to computer authentication weaknesses. DISA estimates that users notice only one in 20 attacks and of these, only one in 20 is reported.¹⁷ Those attacks that do get noticed are perpetrated by novices or the very careless. Rogue nations with experienced, well-financed cyber warriors can attack with virtual immunity. Using *Trojan Horse* versions of programs, hackers can mask process activity, secondary storage and network protocol usage so as to withstand checksum and file-size integrity checks. System administrators will not even know they have been compromised. Unlike the telltale remains of a physical terrorist bomb, there are no bomb fragments in cyberwar, no log of events that can be linked to the attacking nation and no fear of reprisal for destroying a nation's informational architecture. US enemies can attack without fear of being counterattacked. In my opinion, computer authentication is a US security failure, and it might result in grievous damage to US informational infrastructure.

The physical network infrastructure, as well as the civilian encryption standard—Data Encryption Standard (DES)—used throughout the United States present serious security weaknesses. The most dominant media access control network protocol within the United States is *Ethernet*, a simple, easy to manage and easy to compromise protocol. A single user can easily eavesdrop on all traffic on a local segment and can just as easily jam the *Ethernet* segment, thereby crippling the link. Depending on router configuration and protocol usage, this jamming could easily paralyze the entire metropolitan area network through programmed broadcast "storms" using Microsoft's *NETBEUI* protocol—one of the world's most popular protocols. By attacking from several locations simultaneously, it is almost impossible to determine the source of the attack.

Although other protocols such as *FDDI* and *Token Ring* address these security issues by limit-

ing access and the traffic load generated by an individual station and can easily foil traffic-analysis attacks, these protocols enjoy limited use in local

The physical network infrastructure, as well as the civilian encryption standard—Data Encryption Standard (DES)—used throughout the United States present serious security weaknesses. The most dominant media access control network protocol within the United States is Ethernet, a simple, easy to manage and easy to compromise protocol

Like the protocol of parking planes in neat, tight rows at Pearl Harbor, the extensive use of Ethernet makes perfect sense until there is a cyberwar attack. But unlike changing the airplane parking protocol at Pearl Harbor, changing network protocols to more secure forms will take man-years of effort and cannot be accomplished overnight.

Ethernet is a fundamental cyberwar weakness—a weakness that our enemies will undoubtedly exploit.

area networks. Like the protocol of parking planes in neat, tight rows at Pearl Harbor, the extensive use of *Ethernet* makes perfect sense until there is a cyberwar attack. But unlike changing the airplane parking protocol at Pearl Harbor, changing network protocols to more secure forms will take man-years of effort and cannot be accomplished overnight. *Ethernet* is a fundamental cyberwar weakness—a weakness that our enemies will undoubtedly exploit.

Finally, civilian encryption standards, such as DES, are a fundamental weakness. Introduced in 1979, DES is a 56-bit private key that is still the dominant US encryption standard. Criticized widely in 1979 as being too weak, it is totally inadequate today. While the computational power used to break encryption keys has increased over 120-fold and the number of computers has skyrocketed, the encryption standard has remained unchanged. Contests such as the \$10,000 RSA secret-key challenge—using donated, spare computational power to crack DES keys—demonstrate the lack of protection provided by DES.¹⁸ Because 95 percent of military traffic travels over poorly protected civilian links, the military is also open to attack.¹⁹ Again,

As more and more people use computers and Internet computer networks, cyberwar attacks will grow dramatically in number and sophistication. The Defense Information Systems Agency (DISA) estimates that as many as 250,000 attacks may have occurred in 1995. . . . Moreover, sophisticated automated tools with user-friendly interfaces allow novices to attack and rapidly exploit systems without a real understanding of how the attack is delivered. . . . Tools such as Cops and Crack quickly find passwords, file structure permissions and process weaknesses that hackers can exploit to gain access to a system and eventually gain "superuser" access.

while better protection is available, such as public key encryption and multilevel link encryption, it is not widely used outside of the military. Like the

German *Enigma* machine of World War II, our "mail" can be read by our enemies and we will not even know we have been compromised. Encryption weaknesses will be the final nails in our cyberwar coffin.

Given the overwhelming vulnerabilities listed above, one may question why the United States has not already been attacked. The answer is we have been and, in most cases, do not even know we have been compromised. Our enemies are sowing the seeds of compromise and destruction through authentication, network protocol and encryption vulnerabilities now so that in a not-so-distant conflict, those seeds can be harvested with devastating effect. We are on the verge of a digital Pearl Harbor—a cyberwar attack that will forever change the nature of warfare. Like Pearl Harbor, it will catch the United States unprepared and lead to the deaths of thousands of Americans. The difference, this is an attack that could have been prevented. **MR**

NOTES

1. Sun Tzu, *The Art of War*, ed. Samuel B. Griffith (Oxford: Clarendon Press, 1963), 77.

2. John Arquilla and David Ronfeldt, "CyberWar is Coming," *Comparative Strategy*, April-June 1993, 141.

3. *Ibid.*, 146-49. The Carthaginian forces under Hannibal excelled in information warfare (IW) in the 2nd Punic War. Hannibal routinely stationed mirrors on hilltops to keep his leaders apprised of the enemy's movements while denying the enemy the ability to monitor Hannibal's forces. Better communications contributed to a string of victories over a 16-year period, culminating in one of IW's most dramatic uses when Hannibal's relatively small forces destroyed a Roman army almost twice as large at Lake Trasimene. The 13th-century Mongols likewise exploited IW to learn their enemy's exact location while remaining elusive until they attacked. Despite being outnumbered, the Mongols defeated the finest armies of Imperial China, Islam and Christendom. Arrow riders, a sophisticated semaphore system, and an emphasis on decentralized command, coupled with a strategic goal to first destroy an enemy's communications and then attack the enemy's armies piecemeal, combined to give the Mongols battlefield information dominance. In one of their greatest campaigns, a Mongol force of 125,000 destroyed the Khwarizm armies of nearly one million soldiers through IW. More recently, the Normandy invasion and Operation *Desert Storm* represent IW masterpieces. At Normandy, the Allies used the persona of Patton, false units and German *ULTRA* code compromises to deceive German forces about the true location of the invasion and the actual units participating. IW played a large part in destroying the German 7th Army as it moved to counterattack the Allies. During *Desert Storm*, the coalition cut the Iraqi army off from its leadership and then blinded that leadership to the disposition of coalition forces. Furthermore, a force of 20,000 Marines afloat were able to tie down approximately 125,000 Iraqi defenders. The coalition, masterfully employing IW, decimated the 4th-largest army in the world with minimal casualties. There are countless other historical IW accounts which I have omitted due to space constraints. Also, see Gary F. Wheatley and Richard E. Hayes, *Information Warfare and Deterrence*, Advanced Concepts, Technologies and Information Strategies Workshop (December 1996), 61; and Richard Szafarski, "A Theory of Information Warfare: Preparing for 2020," at <<http://www.cdsar.af.mil/apj/szfran.html>>, 7.

4. "Emerging Military Instruments" 1996 *Strategic Assessment* (Washington, DC: National Defense University [NDU] Press, 1996), 188.

5. Martin C. Libicki, *The Mesh and the Net* (Washington, DC: NDU Press, 1995), 11.

6. Ted Eisenberg, David Gries, Juris Harmanis, Don Holcomb, M. Stuart Lynn and Thomas Santoro, "The Computer Worm," *A Report to the Provost of Cornell University on an Investigation Conducted by the Commission of Preliminary Enquiry*, 6 February 1989. See also Eugene H. Spafford, "The Internet Worm Program: An Analysis," *Purdue Technical Report CSD-TR-823*, 8 December 1988; Jon A. Rochlis and Mark W. Eichin, "With Microscope and Tweez-

ers: The Worm from MIT's Perspective," *Communications of the ACM*, June 1989, 689-98; and Eugene H. Spafford, "Crisis and Aftermath: The Internet Worm," *Communications of the ACM*, June 1989, 678-87.

7. E-mail between MAJ Curtis A. Carver Jr. and Dr. Dave Stafford dated 27 July 1992. The attacks featured Trojan Horse PS and LS commands with correct binary checksums that masked attacker files, directories and processes, as well as protocol tunneling to hide network activity.

8. Joint Publication 3-13.1, *Joint Doctrine for Command and Control Warfare*, February 1996. Also see Clifford Stoll, *Cuckoo's Egg* (New York: Doubleday Press, 1989); US Naval Criminal Investigative Service, "Argentine Intrusion Investigation," United States Naval Criminal Investigative Service Slideshow (7 May 1996); and Director of Defense Information Systems Agency, "Information Security: Computer Attacks at Department of Defense Pose Increasing Risks," *Testimony Before the U.S. Senate Permanent Subcommittee on Investigations and Committee of Governmental Affairs* (22 May 1996), 3.

9. *Testimony Before the US Senate Permanent Subcommittee on Investigations and Committee of Governmental Affairs* (22 May 1996), 2.

10. US Naval Criminal Investigative Service, 9.

11. Alex Muffett, "Crack," <<http://ciac.llnl.gov/ciac/ToolsUnixAuth.html>>; and "The Computer Oracle and Password System," <<http://ciac.llnl.gov/ciac/ToolsUnixSysMon.html>>.

12. David Alberts, *Defensive Information Warfare*, (Washington, DC: National Strategic Studies, 1996), 15.

13. Thomas Woo and Simon S. Lam, "Authentication for Distributed Systems," *IEEE Computer* (January 1992), 40.

14. The author and Department of Electrical Engineering and Computer Science UNIX system administrator conducted the password-cracking attempts bi-annually with consistent results of 30-percent account compromise.

15. Of the devices listed, one-time passwords and public key digital signatures offer the best protection and are inexpensive. Biometric devices are still in their infancy and are expensive, offering less than ideal results. As with all security matters, there is a trade-off between security, performance, convenience and system complexity management.

16. J.G. Steiner, C. Neuman and J.I. Schiller, "Kerberos: An Authentication Service for Open Network Systems," *Proceedings of the Winter USENIX Conference* (Berkeley, CA: USENIX Association, 1988), 191-202. See also J.J. Tardo and K. Alagappan, "SPX: Global Authentication Using Public Key Certificates," *Proceedings of IEEE Symposium on Research in Security and Privacy* (Los Alamitos, CA: IEEE CS Press, Order No. 2168, 1991), 232-44.

17. Alberts, 11.

18. RSA Laboratories, "The RSA Secret-Key Challenge," <<http://www.rsa.com/rsalabs/97challenge>>.

19. "Information Warfare: A Two-Edged Sword," *Rand Research Review*, <<http://www.rand.org/publications/RRR/RRRfall95/cyber>>.

Major Curtis A. Carver Jr. is a Ph.D. candidate at Texas A&M University. He received a B.S. from the United States Military Academy (USMA) and an M.S. from Texas A&M. He is a graduate of the US Army Command and General Staff College. He has served in a variety of command and staff positions in the Continental United States, Korea and Italy, to include deputy G6, 2d Infantry Division, Camp Red Cloud, Korea; assistant professor, USMA, West Point, New York; S3, 509th Signal Battalion, Camp Darby, Italy; and commander, 56th Signal Company, Camp Darby.